

# Relative Hulls and Quantum Codes

Sarah E. Anderson, Eduardo Camps-Moreno<sup>1</sup>, Hiram H. López<sup>2</sup>, *Senior Member, IEEE*,  
Gretchen L. Matthews<sup>3</sup>, *Senior Member, IEEE*, Diego Ruano<sup>4</sup>, and Ivan Soprunov<sup>5</sup>

**Abstract**—Given two  $q$ -ary codes  $C_1$  and  $C_2$ , the relative hull of  $C_1$  with respect to  $C_2$  is the intersection  $C_1 \cap C_2^\perp$ . We prove that when  $q > 2$ , the relative hull dimension can be repeatedly reduced by one, down to a certain bound, by replacing either of the two codes with an equivalent one. The reduction of the relative hull dimension applies to hulls taken with respect to the  $e$ -Galois inner product, which has as special cases both the Euclidean and Hermitian inner products. We give conditions under which the relative hull dimension can be increased by one via equivalent codes when  $q > 2$ . We study some consequences of the relative hull properties on entanglement-assisted quantum error-correcting codes and prove the existence of new entanglement-assisted quantum error-correcting maximum distance separable codes, meaning those whose parameters satisfy the quantum Singleton bound.

**Index Terms**—Hull, entanglement-assisted quantum error-correcting codes, CSS construction, quantum codes.  
MSC2010: 94B05; 81P70; 11T71; 14G50.

## I. INTRODUCTION

LET  $C$  be a linear code over a finite field  $\mathbb{F}_q$ . The hull of  $C$  is defined by  $\text{Hull}(C) = C \cap C^\perp$ , where  $C^\perp$  is the dual of  $C$  taken with respect to the Euclidean inner product. Carlet, Mesnager, Tang, Qi, and Pellikaan proved in the seminal paper [8] the existence of LCD codes (codes where the hull is 0) for the case of the Euclidean and the Hermitian inner product when  $q > 3$ . Luo et al. proved in [27] that when  $q > 2$ , the dimension of the Hermitian hull  $\text{Hull}_h(C) = C \cap C^{\perp_h}$ , where  $C^{\perp_h}$  is the Hermitian dual

Manuscript received 29 December 2022; revised 23 December 2023; accepted 19 February 2024. Date of publication 8 March 2024; date of current version 23 April 2024. The work of Hiram H. López was supported in part by NSF under Grant DMS-2201094 and Grant DMS-2401558. The work of Gretchen L. Matthews was supported in part by NSF under Grant DMS-2201075 and in part by the Commonwealth Cyber Initiative. The work of Diego Ruano was supported in part by MICIU/AEI/10.13039/501100011033 and by the “European Union NextGenerationEU/PRTR” under Grant TED2021-130358B-I00, and by MICIU, the European Union NextGenerationEU (PRTR C17.I1) and Junta de Castilla y León under Grant QCAYLE. This work was supported by the National Science Foundation under Grant DMS-1929284. (*Corresponding author: Hiram H. López.*)

Sarah E. Anderson is with the Department of Mathematics, University of St. Thomas, Saint Paul, MN 55105 USA (e-mail: ande1298@stthomas.edu).

Eduardo Camps-Moreno, Hiram H. López, and Gretchen L. Matthews are with the Department of Mathematics, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: eduardoc@vt.edu; hhlopez@vt.edu; gmatthews@vt.edu).

Diego Ruano is with IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain (e-mail: diego.ruano@uva.es).

Ivan Soprunov is with the Department of Mathematics and Statistics, Cleveland State University, Cleveland, OH 44115 USA (e-mail: i.soprunov@csuohio.edu).

Communicated by X. Zhang, Associate Editor for Coding and Decoding.  
Digital Object Identifier 10.1109/TIT.2024.3373550

of  $C$ , can be reduced to zero one by one in the sense that if  $\dim \text{Hull}_h(C) > 0$ , then there exists a code  $C'$  monomially equivalent to  $C$  such that  $\dim \text{Hull}_h(C') = \dim \text{Hull}_h(C) - 1$ . A slight modification reveals the same result for the hull of  $C$  (taken with respect to the Euclidean inner product) when  $q > 3$ . Therefore, there exists a sequence of monomially equivalent codes  $C_0, C_1, \dots, C_t = C$  such that  $\dim \text{Hull}(C_i) = i$ , where  $t = \dim \text{Hull}(C)$ . How equivalent codes can change the hull is also studied in [9].

It is well known that self-orthogonal codes with respect to the Hermitian inner product may be used to construct quantum error-correcting codes [1], [5], [22]. Entanglement allows one to remove restrictions on the relationship between a code and its dual. Hence, any linear code (not necessarily self-orthogonal) may be used to define a quantum code [4]. One may also use two codes  $C_1, C_2 \subseteq \mathbb{F}_q^n$  satisfying  $C_2^\perp \subseteq C_1$  via the now famous CSS construction [6], [37]. In the case of the construction of entanglement-assisted quantum error-correcting codes using linear codes  $C_1, C_2 \subseteq \mathbb{F}_q^n$ , the required number of pairs of maximally entangled qudits is given by the parameter  $c = \dim(C_1) - \dim(C_1 \cap C_2^\perp)$  [39]. Therefore, a key ingredient for computing  $c$  is  $C_1 \cap C_2^\perp$ , which we call the relative hull. More explicitly, the *relative hull of  $C_1$  with respect to  $C_2$*  is

$$\text{Hull}_{C_2}(C_1) = C_1 \cap C_2^\perp.$$

Note that the hull of  $C$  is  $\text{Hull}(C) = \text{Hull}_C(C)$ .

In this paper, we study how equivalent codes change the relative hull. Specifically, we look for codes  $C'_1$  and  $C'_2$  equivalent to  $C_1$  and  $C_2$ , respectively, such that the dimension of  $\text{Hull}_{C'_2}(C'_1)$  is larger or smaller than that of  $\text{Hull}_{C_2}(C_1)$ . We first show that to increase or decrease the relative hull dimension, we only need to find an equivalent code for one of the codes. Then, we show that the relative hull with respect to Galois inner products [12], [23] (which include the Euclidean and Hermitian inner products as particular cases) can be computed in terms of the Euclidean inner product, justifying the focus on the classical Euclidean inner product in this work. One of the main results of this paper is Theorem 3.3, where we show that we can successively decrease the dimension of the relative hull by one via equivalent codes when  $q > 2$ . We provide a similar result for  $e$ -Galois hulls. As a corollary, we can recover the analogous result in [8] for the Euclidean inner product and in [27] for the Hermitian inner product as special cases.

This paper also concerns increasing the relative hull dimension. Proposition 4.5 gives an upper bound for the dimension

of  $\text{Hull}_{C_2}(C_1)$ , which sometimes also is an upper bound for  $\dim \text{Hull}_{C_2}(C'_1)$  for any codes  $C'_1$  and  $C'_2$  equivalent to  $C_1$  and  $C_2$ . Theorem 4.6 shows we can successively increase the dimension of  $\text{Hull}_{C_2}(C_1)$  by one via equivalent codes up to the upper bound given in Proposition 4.5 when  $q > 2$ .

Another primary goal is to apply our results to quantum error-correcting codes. We use the standard notation  $[[n, \kappa, \delta; c]]_q$  to mean that a quantum code  $Q$  is a  $q$ -ary entanglement-assisted quantum error-correcting code (EAQECC) that encodes  $\kappa$  logical qudits into  $n$  physical qudits with the help of  $n - \kappa - c$  ancillas and  $c$  pairs of maximally entangled qudits. The *rate*  $\rho$  and *net rate*  $\bar{\rho}$  of  $Q$  are respectively defined by

$$\rho := \frac{\kappa}{n}, \quad \bar{\rho} := \frac{\kappa - c}{n}.$$

As stated, the relative hull dimension is linked to the required number of pairs of maximally entangled quantum states for an EAQECC. Our results concerning the relative hull demonstrate how monomially equivalent codes may be used to tailor the parameter  $c$  within the specified bounds. Thus, we can reduce the required number of pairs of maximally entangled quantum states while maintaining the net rate. Hence, one has a simpler implementation with the same net rate. We show that if a quantum code obtained via the CSS construction using  $C_1$  and  $C_2$  is pure, then the minimum distance of the quantum code obtained via the CSS construction of some linear codes monomially equivalent to  $C_1$  and  $C_2$  does not decrease. Furthermore, we give conditions to obtain a pure quantum code using monomially equivalent codes. We obtain EAQECCs codes with excellent parameters by applying Theorem 3.3 to multivariate Goppa codes, filling in some gaps or improving the parameters of some of the best-known EAQECCs recently published by Sok [36]. We obtain new EAQMDS (EAQECCs whose parameters achieve the Singleton bound, so-called entanglement-assisted quantum maximum distance separable codes), by applying Theorem 3.3 to (possibly extended or double extended) generalized Reed-Solomon codes when  $q > 2$ ,  $1 < n < q + 1$ , and  $k \leq n + 2$ .

This paper is organized as follows. Preliminaries are given in Section II. Section III provides results on reducing the relative hull while Section IV discusses increasing the relative hull. Applications to the design of entanglement-assisted quantum error-correcting codes are in Section V. The paper ends with a conclusion in Section VI.

## II. PRELIMINARIES

This section provides a foundation for the rest of the paper in terms of preliminary results and notation. Subsection II-A explores the relative hull with respect to the usual (Euclidean) inner product. Subsection II-B introduces the  $e$ -Galois relative hull, the relative hull with respect to the more recently introduced Galois inner products, among which we find the Hermitian inner product. Subsection II-B also proves that the  $e$ -Galois relative hulls are particular cases of the relative hulls with respect to the usual inner product. Subsection II-C reviews the primary constructions of quantum error-correcting codes used in this paper and links them to relative hulls.

### A. Relative Hulls and Code Equivalence

Let  $\mathbb{F}_q$  be the finite field with  $q$  elements. The multiplicative group  $\mathbb{F}_q \setminus \{0\}$  is denoted by  $\mathbb{F}_q^*$ . For  $c \in \mathbb{F}_q^n$ , we denote by  $\text{wt}(c)$  the (Hamming) *weight* of  $c$ , which is the number of nonzero entries of  $c$ . For  $S \subseteq \mathbb{F}_q^n$ , we denote by  $\text{wt}(S)$  the *minimum* of the weights of the elements of  $S \setminus \{0\}$ . A *linear code*  $C$  over  $\mathbb{F}_q$  of length  $n$  is a vector subspace of  $\mathbb{F}_q^n$ ; we may say *code* for short because we only deal with linear codes. An  $[n, k, d]_q$ -code is a linear code over  $\mathbb{F}_q$  of length  $n$ , dimension  $k$  as an  $\mathbb{F}_q$ -subspace, and *minimum distance*  $d(C) = \text{wt}(C)$ ; we sometimes refer to such a code as an  $[n, k]_q$ -code if the minimum distance is irrelevant to the discussion. The *Euclidean dual* of  $C$  is denoted and defined by

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\},$$

where  $x \cdot c = \sum_{i=1}^n x_i c_i$  is the *Euclidean inner product*. Recall that  $\text{Hull}(C) = C \cap C^\perp$ . We say that  $C$  is *self-orthogonal* if  $\text{Hull}(C) = C$  and that  $C$  is *linear complementary dual* (LCD) if  $\text{Hull}(C) = \{0\}$ . The set of  $m \times n$  matrices with entries in  $\mathbb{F}_q$  is denoted by  $\mathbb{F}_q^{m \times n}$ , and  $\text{rk}(M)$  denotes the rank of a matrix  $M \in \mathbb{F}_q^{m \times n}$ . The *kernel* of  $G \in \mathbb{F}_q^{k \times n}$  is  $\ker(G) = \{x \in \mathbb{F}_q^n \mid Gx^T = 0\}$ . The  $j$ -th standard basis vector of  $\mathbb{F}_q^n$  is  $e_j = (0, \dots, 0, 1, 0, \dots, 0)$  where the only nonzero entry is in the  $j$ -th coordinate.

*Definition 2.1:* Let  $C_1$  and  $C_2$  be two codes of the same length over  $\mathbb{F}_q$ . We define the *relative hull of  $C_1$  with respect to  $C_2$*  as

$$\text{Hull}_{C_2}(C_1) = C_1 \cap C_2^\perp.$$

The *hull* of  $C_1$  is  $\text{Hull}(C_1) = \text{Hull}_{C_1}(C_1)$ .

Let  $x$  be an element of  $\text{Hull}_{C_1}(C_2) = C_1^\perp \cap C_2$  and  $c$  an element of  $\text{Hull}_{C_2}(C_1) = C_1 \cap C_2^\perp$ . As  $x \cdot c = 0$ , we conclude that  $\text{Hull}_{C_1}(C_2) \subseteq (\text{Hull}_{C_2}(C_1))^\perp$  (note that  $(A \cap B)^\perp = A^\perp + B^\perp$ ). In particular,  $\text{Hull}(C)$  is a self-orthogonal code for any linear code  $C$ . Note that  $\text{Hull}(C_1) \subseteq \text{Hull}_{C_2}(C_1)$  if  $C_2 \subseteq C_1$  and  $\text{Hull}_{C_2}(C_1) \subseteq \text{Hull}(C_1)$  if  $C_1 \subseteq C_2$ .

The following result presents some basic properties of the relative hull.

*Proposition 2.2:* Let  $C_i$  be an  $[n, k_i]_q$ -code with generator matrix  $G_i$  for  $i = 1, 2$ . The following hold:

(i)  $\text{Hull}_{C_2}(C_1) = \{xG_1 \mid x \in \ker(G_2G_1^T)\},$

(ii)  $\dim \text{Hull}_{C_2}(C_1) = k_1 - \text{rk}(G_2G_1^T),$  and

(iii)  $k_1 - \dim \text{Hull}_{C_2}(C_1) = k_2 - \dim \text{Hull}_{C_1}(C_2).$

*Proof:* (i) ( $\subseteq$ ) If  $c \in \text{Hull}_{C_2}(C_1) = C_1 \cap C_2^\perp$ , then  $c = xG_1$  for some  $x \in \mathbb{F}_q^{k_1}$  and  $G_2c^T = 0$ . Hence,  $G_2G_1^T x^T = 0$ , which means that  $x \in \ker(G_2G_1^T)$ . We conclude that  $c \in \{xG_1 \mid x \in \ker(G_2G_1^T)\}$ .

( $\supseteq$ ) If  $c \in \{xG_1 \mid x \in \ker(G_2G_1^T)\}$  then there is  $x \in \ker(G_2G_1^T)$  such that  $c = xG_1$  indicating that  $c \in C_1$ . Furthermore,  $G_2c^T = G_2G_1^T x^T = 0$ , demonstrating that  $c \in C_2^\perp$ . Thus,  $c \in C_1 \cap C_2^\perp = \text{Hull}_{C_2}(C_1)$ .

(ii) The matrix  $G_1 \in \mathbb{F}_q^{k_1 \times n}$  has rank  $k_1$ , so it defines the injective transformation  $T_{G_1}: \mathbb{F}_q^{k_1} \rightarrow \mathbb{F}_q^n$  given by  $x \mapsto xG_1$ .

Combining this fact with (i) shows

$$\begin{aligned} \dim \text{Hull}_{C_2}(C_1) &= \dim \{xG_1 \mid x \in \ker(G_2G_1^T)\} \\ &= \dim \{x \mid x \in \ker(G_2G_1^T)\} \\ &= \dim \ker(G_2G_1^T) \\ &= k_1 - \text{rk}(G_2G_1^T). \end{aligned}$$

(iii) This is a consequence of  $\text{rk}(G_2G_1^T) = \text{rk}(G_1G_2^T)$  and (ii).  $\square$

A *monomial matrix* is an invertible matrix with rows of weight one. If all nonzero entries of a monomial matrix are ones, it is called a *permutation matrix*.

*Definition 2.3:* Two codes  $C$  and  $C'$  over  $\mathbb{F}_q$  of the same length are *monomially equivalent*, or *equivalent* for short, if there exists a monomial matrix  $M$  such that

$$C' = CM = \{cM \mid c \in C\}.$$

In fact, according to MacWilliams' theorem, every isometry on  $\mathbb{F}_q^n$  with respect to the Hamming metric is given by a monomial matrix [29, Theorem 4]. As monomial equivalence preserves the weight distributions, equivalent codes have the same basic parameters: length, dimension, and minimum distance. It is easy to see that the duals of equivalent codes are equivalent. More precisely,  $C$  and  $C'$  are equivalent with  $C' = CM$  if and only if  $C'^{\perp}$  and  $C^{\perp}$  are equivalent with  $C'^{\perp} = C^{\perp}PD^{-1}$ , where  $M = PD$ ,  $P$  is a permutation matrix, and  $D$  is a nonsingular diagonal matrix.

Given two codes  $C_1, C_2 \subseteq \mathbb{F}_q^n$ , we aim to find equivalent codes that define a relative hull of dimension that is increased or decreased by one from that of the hull of the original codes and then proceed iteratively. More precisely, we are looking for codes  $C'_1$  and  $C'_2$  equivalent to  $C_1$  and  $C_2$ , respectively, such that  $\dim \text{Hull}_{C'_2}(C'_1) = \dim \text{Hull}_{C_2}(C_1) + 1$  or  $\dim \text{Hull}_{C'_2}(C'_1) = \dim \text{Hull}_{C_2}(C_1) - 1$ . The following observation shows that modifying only one of the codes is enough to increase or decrease the relative hull dimension. In other words, when we look for codes  $C'_1$  and  $C'_2$  equivalent to  $C_1$  and  $C_2$  such that  $\dim \text{Hull}_{C'_2}(C'_1) = \dim \text{Hull}_{C_2}(C_1) + 1$  or  $\dim \text{Hull}_{C'_2}(C'_1) = \dim \text{Hull}_{C_2}(C_1) - 1$ , we can always take  $C'_2 = C_2$ .

*Proposition 2.4:* If  $C_i \subseteq \mathbb{F}_q^n$  is a code and  $M_i \in \mathbb{F}_q^{n \times n}$  is a monomial matrix for  $i = 1, 2$ , then

$$\begin{aligned} \dim \text{Hull}_{C_2M_2}(C_1M_1) &= \dim \text{Hull}_{C_2M}(C_1) \\ &= \dim \text{Hull}_{C_2}(C_1M^T), \end{aligned}$$

where  $M = M_2M_1^T$ .

*Proof:* Let  $G_1$  and  $G_2$  be generator matrices for  $C_1$  and  $C_2$ , respectively. By Proposition 2.2 (ii),

$$\begin{aligned} \dim \text{Hull}_{C_2M_2}(C_1M_1) &= k_1 - \text{rk}(G_2M_2(G_1M_1)^T) \\ &= k_1 - \text{rk}(G_2MG_1^T) \\ &= \dim \text{Hull}_{C_2M}(C_1). \end{aligned}$$

Noting that  $G_2MG_1^T = G_2(G_1M)^T$ , we also see that

$$\dim \text{Hull}_{C_2M}(C_1) = \dim \text{Hull}_{C_2}(C_1M^T),$$

which proves the assertion.  $\square$

## B. Hermitian and Galois Relative Hulls

In [12], Fan and Zhang introduced the Galois inner products, a generalization of the Euclidean and Hermitian inner products, and found self-orthogonal codes with respect to the new inner product. The Galois inner products were further studied to build LCD codes [23] and to get new families of quantum codes with a broader range of parameters (see, for example, [7], [24]). This section reviews the Galois inner products and the relative hulls with respect to them. It also demonstrates why, for our purposes, it is sufficient to focus on the classical Euclidean relative hull (rather than these more general Galois relative hulls).

Consider the finite field  $\mathbb{F}_q$ , where  $q = p^m$  for a prime  $p$  and a positive integer  $m$ . For any integer  $e$  such that  $0 \leq e < m$ , the  $e$ -Galois inner product for  $x, y \in \mathbb{F}_q^n$  is given by

$$x \cdot_e y = \sum_{i=1}^n x_i y_i^{p^e} \in \mathbb{F}_q.$$

Taking  $e = 0$  recovers the Euclidean inner product in  $\mathbb{F}_q^n$ . Taking  $e = \frac{m}{2}$  when  $m$  is even produces the usual Hermitian inner product in  $\mathbb{F}_q^n$  that is denoted by  $x \cdot_h y$ . The  $e$ -Galois dual of a code  $C \subseteq \mathbb{F}_q^n$  is defined by

$$C^{\perp_e} = \{x \in \mathbb{F}_q^n \mid x \cdot_e c = 0, \text{ for all } c \in C\}.$$

The *Hermitian dual* is denoted by  $C^{\perp_h}$ . Given two codes  $C_1$  and  $C_2$  over  $\mathbb{F}_q$ , we define the  $e$ -Galois relative hull of  $C_1$  with respect to  $C_2$  as

$$\text{Hull}_{C_2}^e(C_1) = C_1 \cap C_2^{\perp_e}.$$

We denote the *Hermitian relative hull* by  $\text{Hull}_{C_2}^h(C_1)$ . The  $e$ -Galois relative hulls  $\text{Hull}_{C_1}^e(C_1)$  and  $\text{Hull}_{C_1}^h(C_1)$  are denoted respectively by  $\text{Hull}_e(C_1)$  and  $\text{Hull}_h(C_1)$ .

Given a code  $C \subseteq \mathbb{F}_q^n$ , consider the code

$$C^{p^e} = \{(c_1^{p^e}, \dots, c_n^{p^e}) \mid (c_1, \dots, c_n) \in C\}.$$

Since the map  $\mathbb{F}_q \rightarrow \mathbb{F}_q : x \mapsto x^{p^e}$  is bijective, we have that if  $G = [a_{ij}] \in \mathbb{F}_q^{k \times n}$  is a generator matrix of  $C$ , then  $G^{p^e} = [a_{ij}^{p^e}] \in \mathbb{F}_q^{k \times n}$  is a generator matrix of  $C^{p^e}$ . Moreover,

$$C^{\perp_e} = (C^{p^e})^{\perp}.$$

Thus,

$$\begin{aligned} \text{Hull}_{C_2}^e(C_1) &= \text{Hull}_{C_2^{p^e}}(C_1) \\ \text{and} \quad \text{Hull}_e(C) &= \text{Hull}_{C^{p^e}}(C). \end{aligned} \quad (1)$$

Consequently, to consider the relative hull of a code  $C_1$  with respect to  $C_2$  and any  $e$ -Galois inner product, it suffices to consider the relative hull of  $C_1$  with respect to  $C'_2 := C_2^{p^e}$  and the Euclidean inner product.

## C. Quantum Codes

A series of works in the 1990s showed how a self-orthogonal code or two linear codes subject to a dual-containment constraint give rise to quantum error-correcting codes. Since then, many quantum codes in the literature have relied on the dual of a code. In 2006, Brun et al. [4]

demonstrated that the duality requirement could be removed by using the entanglement, paving the way for any linear code or pair of linear codes to design Entanglement-Assisted Quantum Error-Correcting Codes (EAQECCs). The cost of the pre-shared entanglement can affect the analysis of the performance of a code. Thus, looking for constructions with different required numbers of pairs of maximally entangled qudits is valuable. Moreover, EAQECCs have been used recently for secret sharing [34]. Building on the work of Wilde and Brun [39], Guenda et al. [21] showed that the dimension of the hull of the linear code could capture the necessary entanglement. In this subsection, we review the concepts from the recent work [15], [16] that motivate the remainder of this paper.

Recall that the standard notation  $[[n, \kappa, \delta; c]]_q$  describes a quantum code  $Q$  that is a  $q$ -ary EAQECC that encodes  $\kappa$  logical qudits into  $n$  physical qudits with the help of  $n - \kappa - c$  ancillas and  $c$  pairs of maximally entangled qudits; the code is able to detect any error affecting at most  $d - 1$  of the physical qudits. If for any error  $E$  affecting less than  $d$  qudits, we have  $v^T E u = 0$  for any  $v, u \in Q$ , we say that  $Q$  is pure.

There are several constructions of EAQECCs using linear codes. For example, we have the following two classical constructions using the Euclidean and the Hermitian inner products.

*Theorem 2.5 (CSS Construction, [15, Theorem 4]):* If  $C_i$  is an  $[n, k_i]_q$ -code for  $i = 1, 2$ , then there exists an  $[[n, \kappa, \delta; c]]_q$ -quantum code  $Q$  with

$$c = k_1 - \dim \text{Hull}_{C_2}(C_1), \quad \kappa = n - k_1 - k_2 + c,$$

$$\text{and } \delta = \begin{cases} \min \{d(C_1^\perp), d(C_2^\perp)\} & \text{if } C_1^\perp \subseteq C_2 \\ \min \{\text{wt}_1, \text{wt}_2\} & \text{otherwise,} \end{cases}$$

where  $\text{wt}_1 = \text{wt}(C_1^\perp \setminus \text{Hull}_{C_1}(C_2))$  and  $\text{wt}_2 = \text{wt}(C_2^\perp \setminus \text{Hull}_{C_2}(C_1))$ . Moreover, if  $\delta = \min\{d(C_1^\perp), d(C_2^\perp)\}$ , then  $Q$  is pure.

*Theorem 2.6 (Hermitian Construction, [15, Theorem 3]):* If  $C$  is an  $[n, k]_{q^2}$ -code, then there exists an  $[[n, \kappa, \delta; c]]_q$ -quantum code  $Q$  with

$$c = k - \dim \text{Hull}_h(C), \quad \kappa = n - 2k + c, \quad \text{and}$$

$$\delta = \begin{cases} d(C^{\perp h}) & \text{if } C^{\perp h} \subseteq C \\ \min \{\text{wt}(C^{\perp h} \setminus \text{Hull}_h(C))\} & \text{otherwise.} \end{cases}$$

Moreover, if  $\delta = d(C^{\perp h})$ , then  $Q$  is pure.

The following Singleton-type bound holds for the CSS and Hermitian constructions.

*Theorem 2.7 (Singleton-Type Bound [27]):* If  $Q$  is an  $[[n, \kappa, \delta; c]]_q$ -quantum code obtained via the CSS or the Hermitian construction, then

$$2\delta + \kappa \leq n + c + 2.$$

*Remark 2.8:* Let  $C_i$  be an  $[n, k_i]_q$ -code with generator matrix  $G_i$  for  $i = 1, 2$ . Note that Proposition 2.2 (ii) implies that if  $Q$  is a quantum code constructed via the CSS construction using the codes  $C_1$  and  $C_2$ , then the parameter  $c$ , the required number of pairs of maximally entangled quantum

states, can be seen in terms of the generator matrices:

$$c = \text{rk}(G_2 G_1^T) = \text{rk}(G_1 G_2^T).$$

This implies that swapping the role of  $C_1$  and  $C_2$  does not affect the parameters of the resulting quantum code.

### III. REDUCING THE RELATIVE HULL

Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ . This section aims to repeatedly reduce the relative hull dimension  $\text{Hull}_{C_2}(C_1)$  by one using equivalent codes. We use the phrase reduce the (dimension of the) relative hull to mean to determine equivalent codes that define a relative hull of dimension less than that of the original codes. According to Proposition 2.4, we only need to find an equivalent code for one of the linear codes. Thus, we seek a code  $C'_2$  equivalent to  $C_2$  such that  $\dim \text{Hull}_{C'_2}(C_1) = \dim \text{Hull}_{C_2}(C_1) - 1$ .

For any  $\lambda = (\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_q^*)^n$ , we define the diagonal matrix  $D_\lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$ . Let  $C \subseteq \mathbb{F}_q^n$  be a code and  $S_n$  the symmetric group on  $n$  symbols. If  $\sigma \in S_n$ , the image of  $C$  obtained by permuting the entries of every codeword according to  $\sigma$  is denoted by  $C^\sigma$ . The permutation matrix associated with  $\sigma$  is denoted by  $P_\sigma$ .

*Remark 3.1:* Note that  $C^\sigma = \{cP_\sigma \mid c \in C\}$ . Any monomial matrix  $M$  is of the form  $M = D_\lambda P_\sigma$ , for some  $\lambda \in (\mathbb{F}_q^*)^n$  and some permutation  $\sigma \in S_n$ . Thus, any code  $C'$  monomially equivalent to  $C$  is of the form  $C' = CD_\lambda P_\sigma$ .

When equivalent codes reduce the dimension of the relative hull, the following lemma specifies how much the dimension can be reduced.

*Lemma 3.2:* Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ . If  $C'_2$  is equivalent to  $C_2$ , then

$$\dim \text{Hull}_{C'_2}(C_1) \geq \max\{0, k_1 - k_2\}.$$

*Proof:* By Remark 3.1, there exists a monomial matrix  $M$  such that  $C'_2 = C_2 M$ . Let  $G_1$  and  $G_2$  be generator matrices of  $C_1$  and  $C_2$ , respectively. By Proposition 2.2 (ii),  $\dim \text{Hull}_{C'_2}(C_1) = k_1 - \text{rk}(G_2 M G_1^T)$ . The result follows as  $G_2 M G_1^T$  is a  $k_2 \times k_1$  matrix.  $\square$

Lemma 3.2 indicates that the dimension of the relative hull of a code  $C_1$  with respect to  $C_2$  can be reduced (at most) to the difference in dimensions of the two codes, in the case that the difference is nonnegative, by replacing  $C_1$  with an equivalent code.

One of the main results of this section proves that one can repeatedly decrease the dimension of the relative hull by one until it equals the lower bound given by Lemma 3.2.

Recall that the tensor product of matrices  $A = [a_{ij}] \in \mathbb{F}_q^{r \times n}$  and  $B \in \mathbb{F}_q^{m_1 \times m_2}$  is the matrix that is expressed in block form as

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ a_{21}B & \cdots & a_{2n}B \\ \vdots & & \vdots \\ a_{r1}B & \cdots & a_{rn}B \end{pmatrix} \in \mathbb{F}_q^{r m_1 \times n m_2}.$$

For any two matrices  $A \in \mathbb{F}_q^{r \times n}$  and  $B \in \mathbb{F}_q^{n \times s}$ , their (usual) product can be seen as  $AB = \sum_{i=1}^n \text{Col}_i(A) \otimes \text{Row}_i(B)$ ,

where we use  $\text{Col}_i(A)$  (resp.  $\text{Row}_i(A)$ ) to denote the  $i$ -th column (resp. row) of  $A$ . Thus, for  $\lambda \in (\mathbb{F}_q^*)^n$ , we have

$$\begin{aligned} AD_\lambda B &= \sum_{i=1}^n \lambda_i \text{Col}_i(A) \otimes \text{Row}_i(B) \\ &= AB + \sum_{i=1}^n (\lambda_i - 1) \text{Col}_i(A) \otimes \text{Row}_i(B). \end{aligned} \quad (2)$$

If  $P = P_{(ij)}$  is the permutation matrix that interchanges rows  $i$  and  $j$ , then

$$\begin{aligned} APB &= AB \\ &+ (\text{Col}_j(A) - \text{Col}_i(A)) \otimes (\text{Row}_i(B) - \text{Row}_j(B)). \end{aligned} \quad (3)$$

Now, we will successively decrease the dimension of a relative hull, say  $\text{Hull}_{C_2}(C_1)$ , by one via equivalent codes.

**Theorem 3.3:** Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$  with  $q > 2$ . For any  $\ell$  with  $\max\{0, k_1 - k_2\} \leq \ell \leq \dim \text{Hull}_{C_2}(C_1)$ , there exists a code  $C_{2,\ell}$  equivalent to  $C_2$  such that

$$\dim \text{Hull}_{C_{2,\ell}}(C_1) = \ell.$$

Therefore, the dimension of the relative hull of  $C_1$  with respect to  $C_2$  can be repeatedly decreased by one until it is equal to  $\max\{0, k_1 - k_2\}$  by replacing  $C_2$  with an equivalent code.

*Proof:* Define  $\ell_1 = \dim \text{Hull}_{C_2}(C_1)$  and  $\ell_2 = \dim \text{Hull}_{C_1}(C_2)$ . We may assume that  $\text{Hull}_{C_1}(C_2)$  is given by a generator matrix  $[I_{\ell_2} \ A_2]$  where  $I_{\ell_2}$  is an identity matrix of size  $\ell_2$ , since we seek a code equivalent to  $C_2$ . Extend  $[I_{\ell_2} \ A_2]$  to a generator matrix

$$G_2 = \begin{pmatrix} I_{\ell_2} & A_2 \\ 0 & B_2 \end{pmatrix}$$

of  $C_2$ . Similarly, let  $[A_1 \ B_1]$  be a generator matrix of  $\text{Hull}_{C_2}(C_1)$ , where  $A_1$  is of size  $\ell_1 \times \ell_2$ , and

$$G_1 = \begin{pmatrix} A_1 & B_1 \\ D_1 & E_1 \end{pmatrix}$$

is a generator matrix of  $C_1$ . Observe that  $[I_{\ell_2} \ A_2]G_1^T = 0$  and  $[A_1 \ B_1]G_2^T = 0$ , since the first matrix in each product has rows in the dual of the code generated by the second term of each product, then

$$\begin{aligned} G_2 G_1^T &= \begin{pmatrix} A_1^T + A_2 B_1^T & D_1^T + A_2 E_1^T \\ B_2 B_1^T & B_2 E_1^T \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & B_2 E_1^T \end{pmatrix}, \end{aligned}$$

where  $B_2 E_1^T$  is a  $(k_2 - \ell_2) \times (k_1 - \ell_1)$  matrix. By Proposition 2.2 (iii),  $k_2 - \ell_2 = k_1 - \ell_1$ , so  $B_2 E_1^T$  is a square matrix. This, together with Proposition 2.2(ii), implies that  $B_2 E_1^T$  has full rank. The goal is to increase the rank of  $G_2 G_1^T$ , meaning to determine a code equivalent to  $C_2$  with generator matrix  $G'_2$  so that  $\text{rk}(G'_2 G_1^T) > \text{rk}(G_2 G_1^T)$ .

*Case 1:* Assume  $A_1 \neq 0$ . Then there is  $1 \leq j \leq \ell_2$  such that  $\text{Row}_j(G_1^T) \neq 0$ . Set  $\lambda = (1, \dots, 1, \lambda_j, 1, \dots, 1) \in (\mathbb{F}_q^*)^n$  to be the vector with all entries equal to 1 except in position  $j$  where the entry is  $\lambda_j \neq 1$ . By Eq. (2), we have

$$G_2 D_\lambda G_1^T$$

$$\begin{aligned} &= G_2 G_1^T + (\lambda_j - 1) \text{Col}_j(G_2) \otimes \text{Row}_j(G_1^T) \\ &= \begin{pmatrix} (\lambda_j - 1) e_j^T \otimes \text{Row}_j(A_1^T) & (\lambda_j - 1) e_j^T \otimes \text{Row}_j(C_1^T) \\ 0 & B_2 E_1^T \end{pmatrix}. \end{aligned}$$

Observe that  $\text{rk}(G_2 D_\lambda G_1^T) = k_2 - \ell_2 + 1$ , because  $\lambda_j \neq 0, 1$ .

*Case 2:* Assume  $A_1 = 0$ . In this case,  $G_1 = \begin{pmatrix} 0 & B_1 \\ D_1 & E_1 \end{pmatrix}$ .

Recall that  $B_1 \in \mathbb{F}_q^{\ell_1 \times (n - \ell_2)}$  has full rank. After row operations, we may consider that there are  $\ell_1$  integers  $1 \leq i_1 < \dots < i_{\ell_1} \leq n - \ell_2$  such that  $\text{Col}_{i_j}(B_1) = e_j'$  and  $\text{Col}_{i_j}(E_1) = 0$  for  $1 \leq j \leq \ell_1$ .

*Subcase (i):* Assume that for some  $1 \leq j \leq \ell_1$ ,  $\text{Col}_{i_j}(A_2) \neq 0$ . Let  $\nu = \ell_2 + i_j$ . For an element  $\lambda_\nu \in \mathbb{F}_q^*$  such that  $\lambda_\nu \neq 1$ , define  $\lambda = (1, \dots, 1, \lambda_\nu, 1, \dots, 1) \in (\mathbb{F}_q^*)^n$  as the vector with all entries equal to 1 except in position  $\nu$  where the entry is  $\lambda_\nu$ . Then the matrix

$$G_2 D_\lambda G_1^T = \begin{pmatrix} (\lambda_\nu - 1) \text{Col}_{i_j}(A_2) \otimes e_j' & 0 \\ (\lambda_\nu - 1) \text{Col}_{i_j}(B_2) \otimes e_j' & B_2 E_1^T \end{pmatrix}$$

has rank  $k_2 - \ell_2 + 1$ .

*Subcase (ii):* Assume that  $\text{Col}_{i_j}(A_2) = 0$  for all  $1 \leq j \leq \ell_1$ . Let  $P$  be the permutation matrix that interchanges rows 1 and  $\ell_2 + i_1$ . By Eq. (3),

$$\begin{aligned} G_2 P G_1^T &= G_2 G_1^T \\ &+ \begin{pmatrix} -e_1^T \otimes -e_1' & -e_1^T \otimes \text{Row}_1(D_1^T) \\ \text{Col}_{i_1}(B_2) \otimes -e_1' & \text{Col}_{i_1}(B_2) \otimes \text{Row}_1(D_1^T) \end{pmatrix}. \end{aligned}$$

Since the row space of the second term is generated by the row  $(-e_1', \text{Row}_1(D_1^T))$ , then the matrix  $G_2 P G_1^T$  has rank  $k_2 - \ell_2 + 1$ .

Take  $G'_2 = G_2 P$ . Then  $C_2$  is equivalent to the code  $C'_2$  with generator matrix  $G'_2$ . Moreover, in any case,

$$\text{rk}(G'_2 G_1^T) = \text{rk}(G_2 G_1^T) + 1.$$

According to Proposition 2.2(ii),

$$\begin{aligned} \dim \text{Hull}_{C'_2}(C_1) &= k_1 - \text{rk}(G'_2 G_1^T) \\ &= k_1 - (\text{rk}(G_2 G_1^T) + 1) \\ &= \dim \text{Hull}_{C_2}(C_1) - 1, \end{aligned}$$

meaning we have decreased the dimension  $\dim \text{Hull}_{C_2}(C_1)$  of the relative hull by one. We can continue this process until the rank of the matrix  $G_2 P G_1^T$  is  $k_2$ , which means  $\dim \text{Hull}_{C'_2}(C_1) = \max\{0, k_1 - k_2\}$ .  $\square$

Algorithm 2 captures the procedure written in the proof of Theorem 3.3. The input and the output are given in terms of the generator matrices of the pair of codes. To simplify this algorithm, we first use Algorithm 1 so that the generator matrices are of the appropriate form.

We now give some examples to illustrate how the proof of Theorem 3.3 constructs equivalent codes that reduce the relative hull, using [2], [3], [20] to make the computations.

*Example 3.4:* Let  $a$  be a primitive element of  $\mathbb{F}_9$ , with  $a^2 - a - 1 = 0$ , and  $C_1$  and  $C_2$  the codes over  $\mathbb{F}_9$  generated respectively by

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & a \\ 0 & 1 & 0 & 0 & -a-1 & -a-1 & a \\ 0 & 0 & 1 & 0 & a+1 & a+1 & a+1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

**Algorithm 1** Systematic-Like Form for the Generator Matrices

---

**Data:**  $G_1 \in \mathbb{F}_q^{k_1 \times n}$ ,  $G_2 \in \mathbb{F}_q^{k_2 \times n}$  full-rank matrices.  
**Result:**  $G'_1 \in \mathbb{F}_q^{k_1 \times n}$ ,  $G'_2 \in \mathbb{F}_q^{k_2 \times n}$

- 1  $(k_1, k_2) \leftarrow (\text{rk } G_1, \text{rk } G_2)$
- 2  $(\ell_1, \ell_2) \leftarrow (k_1 - \text{rk}(G_2 G_1^T), k_2 - \text{rk}(G_2 G_1^T))$
- 3 For  $i = 1, 2$ , pick  $M_i \in \mathbb{F}_q^{k_i \times k_i}$  be a non-singular matrix such that the first  $\ell_i$  rows are in  $\ker(G_{1+(i\%2)} G_i^T)$ .
- 4  $(G_1, G_2) \leftarrow (M_1 G_1, M_2 G_2)$
- 5 Pick  $M_3$  a non-singular matrix,  $P$  a permutation matrix such that  $(M_3)_{i,j} = 0$  if  $i \leq \ell_2$  and  $j \geq \ell_2$ , and  $M_3 G_2 P = \begin{pmatrix} I_{\ell_2} & A_2 \\ 0 & B_2 \end{pmatrix}$ .
- 6 Let  $M_4$  be a non-singular matrix such that  $(M_4)_{i,j} = 0$  if  $i \leq \ell_1$  and  $j \geq \ell_1$  and  $M_4 G_1$  is in row-reduced-echelon form.
- 7  $G'_1 \leftarrow M_4 G_1$
- 8  $G'_2 \leftarrow M_3 G_2 P$

---

and

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 & -a-1 & a \\ 0 & 0 & 1 & 0 & a-1 & -a-1 & a \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

The subspaces  $\text{Hull}_{C_2}(C_1)$  and  $\text{Hull}_{C_1}(C_2)$  are generated by the first three rows of  $G_1$  and  $G_2$ , respectively. This example corresponds to the proof of Theorem 3.3, Case 1. We only need to choose  $\lambda$  with entries different from 1 since the first three entries of the main diagonal are non-zero.

For  $0 \leq \ell \leq 3$ , let  $\lambda^{(\ell)} \in \mathbb{F}_9^7$  be the vector such that  $(\lambda^{(\ell)})_i = a$  for  $1 \leq i \leq 3 - \ell$  and  $(\lambda^{(\ell)})_i = 1$  for  $i \geq 3 - \ell$ . Let  $C_{2,\ell}$  be the code generated by  $G_2 D_{\lambda^{(\ell)}}$ . We have

$$G_2 D_{\lambda^{(\ell)}} G_1^T = \begin{pmatrix} \lambda_1^{(\ell)} - 1 & 0 & 0 & 0 \\ 0 & \lambda_2^{(\ell)} - 1 & 0 & 0 \\ 0 & 0 & \lambda_3^{(\ell)} - 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore,  $\text{rk}(G_2 D_{\lambda^{(\ell)}} G_1^T) = 4 - \ell$  and thus  $\dim \text{Hull}_{C_{2,\ell}}(C_1) = \ell$ .

*Example 3.5:* Let  $a$  be a primitive element of  $\mathbb{F}_9$ , with  $a^2 - a - 1 = 0$ , and  $C_1$  and  $C_2$  the codes over  $\mathbb{F}_9$  generated respectively by

$$G_1 = \begin{pmatrix} 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ -a & 0 & 1 & 0 & 0 & 0 \\ 0 & -a-1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 1 & 0 & a & a & 0 & 0 \\ 0 & 1 & 0 & 0 & a+1 & a+1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

The relative hulls are generated by the first two columns of each matrix. As  $G_1$  has its principal minor of size 2 equal to zero, this example corresponds to the proof of Theorem 3.3,

**Algorithm 2** Reducing the Hull of Two Codes

---

**Data:**  $G_1 \in \mathbb{F}_q^{k_1 \times n}$ ,  $G_2 \in \mathbb{F}_q^{k_2 \times n}$  full-rank matrices.  
**Result:**  $G'_2$  a full-rank matrix with  $\text{rk}(G_1 (G'_2)^T) = \text{rk}(G_1 G_2^T) + 1$ .

- 1 Replace  $(G_1, G_2)$  with the result of Algorithm 1.
- 2 **if**  $[(G_1)_{ij}]_{i,j=1}^{\ell_1} \neq 0$  **then**
- 3      $j \leftarrow \min\{h \in [\ell_1] : \exists i \in [\ell_1], (G_1)_{ij} \neq 0\}$
- 4     Take  $\lambda_j \in \mathbb{F}_q \setminus \{0, 1\}$ .
- 5      $\lambda \leftarrow \lambda_j e_j + \sum_{i \in [n] \setminus \{j\}} e_i$
- 6      $G'_2 \leftarrow G_2 D_\lambda$
- 7 **else**
- 8     **if**  $\exists j \in [n]$  such that  $\text{wt}(\text{Col}_j(G_1)) = 1$  and  $\text{Col}_j(G_2) \neq 0$  **then**
- 9         Take  $\lambda_j \in \mathbb{F}_q \setminus \{0, 1\}$ .
- 10          $\lambda \leftarrow \lambda_j e_j + \sum_{i \in [n] \setminus \{j\}} e_i$
- 11          $G'_2 \leftarrow G_2 D_\lambda$
- 12     **else**
- 13         Take  $j \in [n]$  such that  $\text{Col}_j(G_1) = e_1$ .
- 14         Take  $P'$ , the permutation matrix that permutes rows 1 and  $j$ .
- 15          $G'_2 \leftarrow G_2 P'$
- 16     **end**
- 17 **end**

---

Case 2. We can use the first two entries of the last four columns of  $G_2$  to modify the hull size (Subcase (i)) because they are non-zero. Let  $\lambda^{(1)} \in \mathbb{F}_9^6$  such that  $\lambda_i^{(1)} = 1$  for  $i \neq 6$  and  $\lambda_6^{(1)} = a$ . Let  $C_{2,1}$  be the code generated by  $G_2 D_{\lambda^{(1)}}$ . The matrix

$$G_2 D_{\lambda^{(1)}} G_1^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -a+1 & 0 & 1 \end{pmatrix}$$

has rank 3 and  $\dim \text{Hull}_{C_{2,1}}(C_1) = 1$ . We can check that the last three rows of  $G_2$  do not belong to  $\text{Hull}_{C_1}(C_{2,1})$ , so we are still in Case 2, Subcase (i) of the proof of Theorem 3.3. Let  $\lambda^{(2)} \in \mathbb{F}_9^6$  such that  $\lambda_i^{(2)} = 1$  for  $i \neq 4$  and  $\lambda_4^{(2)} = a$ . Let  $C_{2,2}$  be the code generated by  $G_2 D_{\lambda^{(1)}} D_{\lambda^{(2)}}$ . The matrix

$$G_2 D_{\lambda^{(1)}} D_{\lambda^{(2)}} G_1^T = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ -a+1 & 0 & 1 & 0 \\ 0 & -a+1 & 0 & 1 \end{pmatrix}$$

has rank 4 and  $\dim \text{Hull}_{C_{2,2}}(C_1) = 0$ .

*Example 3.6:* Let  $a$  be a primitive element of  $\mathbb{F}_9$ , with  $a^2 - a - 1 = 0$ , and  $C_1$  and  $C_2$  the codes over  $\mathbb{F}_9$  generated respectively by

$$G_1 = \begin{pmatrix} 0 & 0 & -a & -a & 1 & 0 \\ 0 & 0 & -a & -a & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & a & a \\ 0 & 0 & 0 & 1 & a & a \end{pmatrix}.$$

The relative hulls are generated by the first two rows of each matrix. The principal minor of size 2 of  $G_1$  is 0, so this example corresponds to the proof of Theorem 3.3, Case 1. Since the  $(G_2)_{i,j} = 0$  for  $i = 1, 2$  and  $3 \leq j \leq 6$ , we are in the Subcase (ii). We need to perform some column permutations to  $G_2$  to get an equivalent code with a smaller relative hull than  $C_2$ .

Let  $P_1$  be the permutation matrix that permutes columns 5 and 1, and let  $C_{2,1}$  be the code generated by  $G_2P_1$ . The matrix

$$G_2P_1G_1^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -a & 0 & 1 & 0 \\ -a & 0 & 0 & 1 \end{pmatrix}$$

has rank 3, therefore  $\dim \text{Hull}_{C_{2,1}}(C_1) = 1$ .

Let  $P_2$  be the permutation matrix that permutes columns 2 and 6, and let  $C_{2,0}$  be the code generated by  $G_2P_1P_2$ . The matrix

$$G_2P_1P_2G_1^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -a & -a & 1 & 0 \\ -a & -a & 0 & 1 \end{pmatrix}$$

has rank 4 and thus,  $\dim \text{Hull}_{C_{2,0}}(C_1) = 0$ .

Let  $C_1$  and  $C_2$  be two codes over  $\mathbb{F}_q$  with  $q = p^m > 2$ , and let  $e$  be an integer such that  $0 \leq e < m$ . Applying Theorem 3.3 to the relative hull of  $C_1$  with respect to  $C_2^{p^e}$ , we obtain a similar result for the  $e$ -Galois hull of  $C_1$  with respect to  $C_2$ . This consequence is captured in the next statement.

*Corollary 3.7:* Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$  with  $q = p^m > 2$ . Take  $e$  such that  $0 \leq e < m$ . For any  $\ell$  with  $\max\{0, k_1 - k_2\} \leq \ell \leq \dim \text{Hull}_{C_2^e}(C_1)$ , there is a code  $C_{2,\ell}$  equivalent to  $C_2$  such that

$$\dim \text{Hull}_{C_{2,\ell}^e}(C_1) = \ell.$$

Therefore, the dimension of the  $e$ -Galois relative hull of  $C_1$  with respect to  $C_2$  can be repeatedly decreased by one until it is equal to  $\max\{0, k_1 - k_2\}$  by replacing  $C_2$  with an equivalent code.

*Proof:* This statement follows immediately from Theorem 3.3 and Eq. (1).  $\square$

Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ . If  $c_1 = (c_{11}, c_{12}, \dots, c_{1n}) \in C_1$  and  $c_2 = (c_{21}, c_{22}, \dots, c_{2n}) \in C_2$ , then their *Schur product* is defined by

$$c_1 \star c_2 = (c_{11}c_{21}, c_{12}c_{22}, \dots, c_{1n}c_{2n}) \in \mathbb{F}_q^n.$$

The Schur product of the codes  $C_1$  and  $C_2$ , denoted by  $C_1 \star C_2$ , is defined as the  $\mathbb{F}_q$ -vector space spanned by the set  $\{c_1 \star c_2 \mid c_1 \in C_1, c_2 \in C_2\}$ . For an element  $\lambda$  in  $\mathbb{F}_q^n$ ,  $\lambda \star C_2$  denotes the  $\mathbb{F}_q$ -vector space spanned by the set  $\{\lambda \star c_2 \mid c_2 \in C_2\}$ .

*Proposition 3.8:* Let  $C \subseteq \mathbb{F}_q^n$  be a code with  $q = p^m > 2$ . Take  $e$  such that  $0 \leq e < m$  and define  $\ell = \dim \text{Hull}_e(C)$ . If there exists  $x \in \mathbb{F}_q^*$  such that  $x^{p^e+1} \neq 1$ , then  $\dim \text{Hull}_e(\lambda \star C) = \ell - 1$  for some  $\lambda \in (\mathbb{F}_q^*)^n$ .

*Proof:* Let  $G$  be a generator matrix of  $C$ . As  $C^{\perp_e} = (C^{p^e})^\perp$ ,

$$\dim \text{Hull}_e(\lambda \star C) = \dim C - \text{rk}(GD_{\lambda^{p^e+1}}(G^{p^e})^T),$$

where  $(G^{p^e})_{ij} = (G_{ij})^{p^e}$ . The proof of Theorem 3.3 guarantees that we can reduce the rank of this matrix as long as there exists  $x \in \mathbb{F}_q$  with  $x^{p^e+1} \neq 1$ .  $\square$

As a corollary, we can prove some of the significant results that were initially proved by Carlet et al. (existence of LCD codes for the case of the Euclidean and the Hermitian inner product [8]) and Luo et al. (the step-wise reduction of the dimension of the Hermitian hull [27]).

*Corollary 3.9:* Let  $C \subseteq \mathbb{F}_q^n$  be a linear code. The following hold:

- 1) If  $q > 3$  and  $0 \leq \ell \leq \dim \text{Hull}(C)$ , then there is a code  $C_\ell$  equivalent to  $C$  such that  $\text{Hull}(C_\ell) = \ell$ .
- 2) If  $q > 4$  is a square and  $0 \leq \ell \leq \dim \text{Hull}_h(C)$ , then there is a code  $C_\ell$  equivalent to  $C$  such that  $\text{Hull}_h(C_\ell) = \ell$ .

*Proof:* The Euclidean hull is the  $e$ -Galois hull with  $e = 0$ . Thus, it is enough to guarantee that  $x^2 - 1 \neq 0$  for some  $x \in \mathbb{F}_q^*$ , which happens if  $q > 3$ .

The Hermitian hull is also an  $e$ -Galois hull where  $e$  satisfies  $p^e = \sqrt{q}$  and  $p$  is the characteristic of the field. By Proposition 3.8, we can reduce the hull using an equivalent code as long as there is  $x \in \mathbb{F}_q^*$  such that  $x^{\sqrt{q}+1} \neq 1$ . Note that as  $q > 4$ ,  $\sqrt{q} + 1 < q - 1$ . Thus, not all the elements of  $\mathbb{F}_q^*$  can be roots of the polynomial  $f(t) = t^{\sqrt{q}+1} - 1$ , meaning that there is  $x \in \mathbb{F}_q^*$  such that  $x^{\sqrt{q}+1} \neq 1$ . Another way to see this is by noticing that  $x^{\sqrt{q}+1}$  is the norm of  $x$  with respect to the extension  $\mathbb{F}_q/\mathbb{F}_{\sqrt{q}}$ . As the norm is surjective, there are non-zero elements with a norm different from 1 when  $q > 4$ .  $\square$

*Remark 3.10:* If we only consider monomial matrices of the form  $M = D_\lambda$  in the definition of equivalent codes, meaning no permutations of coordinates are allowed, then it may be impossible to reduce  $\dim \text{Hull}_{C_2}(C_1)$  to  $\max\{0, k_1 - k_2\}$ . The following example illustrates this fact.

*Example 3.11:* Let  $C_1$  and  $C_2$  be the codes over  $\mathbb{F}_q$  generated respectively by

$$G_1 = (1 \ 1 \ 0 \ 0) \quad \text{and} \quad G_2 = (0 \ 0 \ 1 \ 1).$$

Note that  $\max\{0, k_1 - k_2\} = 0$  and that  $G_1D_\lambda G_2^T = 0$  for any  $\lambda \in (\mathbb{F}_q^*)^n$ . Hence,  $\dim \text{Hull}_{C_2D_\lambda}(C_1) = 1$  for any  $\lambda \in (\mathbb{F}_q^*)^n$ .

To get the minimum possible hull, we need permutations. If  $P$  is the permutation matrix that interchanges the first and the fourth column, then  $G_1P^T G_2^T = I_1$  and thus  $\text{Hull}_{C_2P}(C_1) = 0$ .

#### IV. INCREASING THE RELATIVE HULL

Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ . In this section, we give conditions that allow us to find equivalent codes that successively increase the dimension of the relative hull of  $C_1$  with respect to  $C_2$  by one. As in Section III, according to Proposition 2.4, we only need to show that an equivalent code exists for one of the linear codes. Hence, we aim to determine when it is possible to find a code  $C'_1$  equivalent to  $C_1$  such that  $\dim \text{Hull}_{C_2}(C'_1) = \dim \text{Hull}_{C_2}(C_1) + 1$ .

The following lemma gives an upper bound on the increased dimension of the relative hull. However, as we will see, it is

only possible sometimes to increase the dimension of the relative hull using equivalent codes.

*Lemma 4.1:* Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ . If  $C'_1$  is equivalent to  $C_1$ , then

$$\dim \text{Hull}_{C_2}(C'_1) \leq \min\{k_1, n - k_2\}.$$

*Proof:* This is clear by the definition of  $\text{Hull}_{C_2}(C'_1)$ .  $\square$

By Theorem 3.3, we can decrease the relative hull dimension by increasing the rank of the matrix  $G_1 G_2^T$ . To increase the relative hull dimension instead, we could try to mimic this idea by decreasing the rank of the matrix  $G_1 G_2^T$  until it is equal to 0. Unfortunately, the following example shows that reducing the rank of this matrix  $G_1 G_2^T$  is not always possible.

*Example 4.2:* Let  $C_1$  and  $C_2$  be the codes over  $\mathbb{F}_q$  generated respectively by

$$G_1 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

For any permutation matrix  $P$  and for any  $\lambda \in (\mathbb{F}_q^*)^4$ , the second column of  $G_1 D_\lambda P G_2^T$  is either  $\pm(\lambda_2 0)^T$  or  $\pm(0 \lambda_2)^T$ . Thus, the rank of  $G_1 D_\lambda P G_2^T$  is at least 1.

We can relate the maximum dimension of the hull under isometries of the form  $D_\lambda$  with the dual of the Schur product of the codes.

*Proposition 4.3:* If  $C_i$  is an  $[n, k_i]_q$ -code for  $i = 1, 2$ , then

$$\begin{aligned} & \max\{\dim \text{Hull}_{C_2}(C_1 D_\lambda) \mid \lambda \in (\mathbb{F}_q^*)^n\} \\ & \geq \max \text{wt}((C_1 \star C_2)^\perp) - n + \min\{k_1, k_2\}. \end{aligned}$$

*Proof:* Let  $G_1$  and  $G_2$  be generator matrices of  $C_1$  and  $C_2$ , respectively. According to Proposition 2.2 (ii), we need to show that

$$\begin{aligned} & \min\{\text{rk}(G_1 D_\lambda G_2^T) \mid \lambda \in (\mathbb{F}_q^*)^n\} \\ & \leq n - \max \text{wt}((C_1 \star C_2)^\perp). \end{aligned}$$

Suppose  $\max \text{wt}((C_1 \star C_2)^\perp) = n - \ell$ , and take  $\gamma \in (C_1 \star C_2)^\perp$  with  $\text{wt}(\gamma) = n - \ell$ . If  $\ell \geq \min\{k_1, k_2\}$ , the result follows as  $\text{rk}(G_1 D_\lambda G_2^T) \leq \min\{k_1, k_2\}$  for any  $\lambda \in (\mathbb{F}_q^*)^n$ . Assume that  $\ell < \min\{k_1, k_2\}$ . Without loss of generality, we can assume that the first  $\ell$  entries of  $\gamma$  are equal to zero. Define  $\lambda = (1, \dots, 1, \gamma_{\ell+1}, \dots, \gamma_n)$ . Then

$$G_1 D_\lambda G_2^T = \left( \sum_{h=1}^{\ell} a_{ih} b_{jh} \right)_{i,j=1}^{k_1, k_2} = G_1 \begin{pmatrix} I_\ell & 0 \\ 0 & 0 \end{pmatrix} G_2^T.$$

Since  $\ell < \min\{k_1, k_2\}$ , the rank of this product is at most  $\ell$ , and we have the conclusion.  $\square$

In the case where  $C_1 = C_2$ , the code  $(C_1 \star C_2)^\perp$  was used in [31] to find self-orthogonal truncations of  $C_1$ .

It is evident that the bound given by Proposition 4.3 is sharp for codes  $C_1$  and  $C_2$  such that there is an equivalent code  $C'$  to  $C_1$  with  $C_2^\perp \subseteq C'$ . The following example shows that the bound may be sharp even when such an equivalent code does not exist.

*Example 4.4:* Take  $G_1 = G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \beta \end{pmatrix} \in \mathbb{F}_q^{2 \times 3}$  with  $\beta \neq 0$ . For any  $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in (\mathbb{F}_q^*)^3$ , we have

$$G_1 D_\lambda G_2^T = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 + \beta^2 \lambda_3 \end{pmatrix}.$$

Then,  $\text{rk}(G_1 D_\lambda G_2^T) = 1$  when  $\lambda_2 = -\beta^2 \lambda_3$ ; otherwise,  $\text{rk}(G_1 D_\lambda G_2^T) = 2$ . Since 1 is the smallest rank achievable for any  $\lambda$ , the maximum rank of the relative hull is  $2 - 1 = 1$ .

On the other hand, if  $C$  is the code generated by  $G_1$ , then a generator matrix for the code  $C \star C$  is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \beta^2 \end{pmatrix}.$$

It is clear that  $(C \star C)^\perp = \langle (0, -\beta^2, 1) \rangle$ . Then

$$\max \text{wt}((C \star C)^\perp) - n + k_1 = 2 - 3 + 2 = 1,$$

demonstrating that equality is achievable in Proposition 4.3.

The bound of Proposition 4.3 is an upper bound for the dimension of the relative hull.

*Proposition 4.5:* If  $C_i$  is an  $[n, k_i]_q$ -code for  $i = 1, 2$ , and  $k_1 \leq k_2$ , then

$$\dim \text{Hull}_{C_2}(C_1) \leq \max \text{wt}((C_1 \star C_2)^\perp) - n + k_1.$$

*Proof:* Let  $G_1$  and  $G_2$  be generator matrices of  $C_1$  and  $C_2$ , respectively, such that

$$G_1 G_2^T = \begin{pmatrix} 0 & 0 \\ 0 & I_\ell \end{pmatrix},$$

where  $\ell$  is defined as  $k_1 - \dim \text{Hull}_{C_2}(C_1)$ . Since a basis for  $C_1 \star C_2$  is given by the set  $\{\text{Row}_i(G_1) \star \text{Row}_j(G_2) : i = 1, \dots, k_1, j = 1, \dots, k_2\}$ , then  $\lambda = \sum_{i \in [n-\ell]} e_i \in (C_1 \star C_2)^\perp$ , and the conclusion follows.  $\square$

The summary of these results is the following theorem.

*Theorem 4.6:* Let  $C_i$  be an  $[n, k_i]_q$ -code with  $q > 2$  for  $i = 1, 2$ . For any  $\ell$  with  $\max\{0, k_1 - k_2\} \leq \ell \leq \max \text{wt}((C_1 \star C_2)^\perp) - n + k_1$ , there exists a code  $C_{1,\ell}$  equivalent to  $C_1$  such that

$$\dim \text{Hull}_{C_2}(C_{1,\ell}) = \ell.$$

In particular, if  $\max \text{wt}((C_1 \star C_2)^\perp) = \min\{n, 2n - k_2 - k_1\}$ ,  $\ell$  runs over all the possible values of  $\dim \text{Hull}_{C_2}(C'_1)$ , where  $C'_1$  is a code equivalent to  $C_1$ .

*Proof:* The result follows from Proposition 4.3, Theorem 3.3, and Lemma 4.1.  $\square$

*Remark 4.7:* We remark that an algorithm for increasing the relative hull would require finding a codeword in  $(C_1 \star C_2)^\perp$  of appropriate weight. Provided such a word can be found, one can implement an algorithm similar to Algorithm 2.

We can find a worse but easier-to-compute lower bound on the maximum rank of the relative hull by using a bound from [32] on optimal anticodes.

*Lemma 4.8 [32]:* If  $C \subseteq \mathbb{F}_q^n$  is a linear code, then  $\dim_{\mathbb{F}_q}(C) \leq \max \text{wt}(C)$ .

A code  $C \subseteq \mathbb{F}_q^n$  with  $\dim_{\mathbb{F}_q}(C) = \max \text{wt}(C)$  is said to be an *optimal linear anticode*.

*Corollary 4.9:* If  $C_i$  is an  $[n, k_i]_q$ -code for  $i = 1, 2$ , and  $k_1 \leq k_2$ , then

$$\max\{\dim \text{Hull}_{C_2}(C_1 D_\lambda) \mid \lambda \in (\mathbb{F}_q^*)^n\} \geq k_1 - \dim(C_1 \star C_2).$$

*Proof:* By Lemma 4.8,  $\dim(C_1 \star C_2)^\perp \leq \max \text{wt}(C_1 \star C_2)^\perp$ . Thus, Proposition 4.3 gives the conclusion.  $\square$

*Remark 4.10:* Assume that  $q \neq 2$ . An optimal anticode of dimension  $k$  is permutation equivalent to  $\mathbb{F}_q^k \oplus \{0\}^{n-k}$ ; see [32] for details. Moreover, the dual of an optimal anticode is an optimal anticode. Consequently, the bound in Corollary 4.9 can only be met if  $(C_1 \star C_2)^\perp$  is an optimal anticode, which implies  $C_1 \star C_2$  is an optimal anticode. Thus, the minimum rank of  $G_1 D_\lambda G_2^T$  equals the maximum weight of  $C_1 \star C_2$ .

## V. APPLICATIONS TO QUANTUM CODES

Many quantum code constructions focus on creating codes that do not require entanglement assistance or pairs of maximally entangled quantum states. However, more recently, propagation rules to construct quantum codes have been established [27], [28]. Luo et al. constructed in [27] new quantum codes with reduced length by increasing the parameter  $c$  and using the Hermitian construction of Theorem 2.5. Luo et al. also gave three new propagation rules related to entanglement using the Hermitian construction in [28]. The first rule increases the parameter  $c$  while increasing the dimension, the second rule keeps  $c$  unchanged while increasing the length, and the third rule decreases  $c$  while increasing the length.

We now state some results that are consequences of the previous sections.

*Theorem 5.1:* Let  $C_i$  be an  $[n, k_i]_q$ -code for  $i = 1, 2$ , with  $q > 2$  and  $k_1 \leq k_2$ . For any integer  $c$  with  $k_1 - \dim(C_1 \cap C_2^\perp) \leq c \leq k_1$ , there is an  $[[n, \kappa, \delta; c]]_q$  quantum code  $Q$  with

$$\kappa = n - k_1 - k_2 + c \quad \text{and} \quad \delta \geq \min\{d(C_1^\perp), d(C_2^\perp)\}.$$

Moreover, if  $\delta = \min\{d(C_1^\perp), d(C_2^\perp)\}$ , then  $Q$  is pure.

*Proof:* We obtain the result using Theorem 3.3 and the CSS construction given in Theorem 2.5.  $\square$

Let  $Q$  be the quantum code obtained via the CSS construction using  $C_1$  and  $C_2$  and  $\delta(Q) = \min\{\text{wt}(C_1^\perp \setminus C_2), \text{wt}(C_2^\perp \setminus C_1)\}$ , where we denote  $C_1^\perp \setminus (C_2 \cap C_1^\perp)$  by  $C_1^\perp \setminus C_2$  for the sake of simplicity. In general, if we take the quantum code  $Q'$  constructed via the CSS construction using  $C_1$  and  $C_2'$ , where  $C_2'$  is equivalent to  $C_2$  and  $C_1 \cap C_2'^\perp = \{0\}$ , then  $\delta(Q') = \min\{\text{wt}(C_1^\perp \setminus C_2'^\perp), d(C_2'^\perp)\}$ . If  $Q$  is not pure, it is possible that  $\delta(Q) \geq \delta(Q')$  since the equivalence can worsen the minimum distance. Otherwise, we have the following result.

*Proposition 5.2:* Let  $Q$  be the pure quantum code obtained via the CSS construction using  $C_1$  and  $C_2$ . If  $Q'$  is a quantum code obtained via the CSS construction using  $C_1$  and a monomially equivalent code  $C_2'$  to  $C_2$ , then  $\delta(Q') \geq \delta(Q)$ .

*Proof:* As  $Q$  is pure, we obtain that  $\delta(Q) = \min\{d(C_1^\perp), d(C_2^\perp)\}$ . Note that  $\delta(Q') = \min\{\text{wt}(C_1^\perp \setminus C_2'^\perp), \text{wt}(C_2'^\perp \setminus C_1)\} \geq \min\{d(C_1^\perp), d(C_2'^\perp)\} = \delta(Q)$ . Thus, the result follows.  $\square$

If  $d(C_1^\perp) < d(C_2^\perp)$ , the equality in the previous corollary depends on how many minimum weight codewords of  $C_1^\perp$  are outside  $C_2$ . If any code equivalent to  $C_2$  does not contain all minimum weight codewords of  $C_1^\perp$ , then the purity is preserved. The following corollary provides an instance of such constructions.

*Proposition 5.3:* Let  $Q$  be the pure quantum code obtained via the CSS construction using  $C_1$  and  $C_2$ . Assume one of the following conditions holds:

- 1)  $d(C_1^\perp) < \min\{d(C_2), d(C_2^\perp)\}$ .
- 2)  $d(C_1^\perp) = d(C_2^\perp)$  and  $d(C_1^\perp) < \min\{d(C_1), d(C_2)\}$ .

Then, any quantum code  $Q'$  constructed via the CSS construction using  $C_1$  and an equivalent code  $C_2'$  to  $C_2$  is pure and  $\delta(Q') = \delta(Q) = d(C_1^\perp)$ .

*Proof:* As  $Q$  is pure, we obtain that  $\delta(Q) = \min\{d(C_1^\perp), d(C_2^\perp)\}$ . Note that  $\delta(Q') = \min\{\text{wt}(C_1^\perp \setminus C_2'), \text{wt}(C_2'^\perp \setminus C_1)\}$  and  $d(C_2) = d(C_2')$ .

*Assume (1):* As  $d(C_1^\perp) < d(C_2)$ , all codewords of minimum weight in  $C_2'$  are outside of  $C_1'$ . Thus,  $\text{wt}(C_1^\perp \setminus C_2') = d(C_1^\perp)$ . As  $d(C_1^\perp) < d(C_2^\perp) = d(C_2'^\perp) < d(C_2'^\perp \setminus C_1)$ , we obtain  $\delta(Q') = \min\{\text{wt}(C_1^\perp \setminus C_2'), \text{wt}(C_2'^\perp \setminus C_1)\} = d(C_1^\perp) = \delta(Q)$ .

*Assume (2):* As  $d(C_1^\perp) < d(C_2)$ , all codewords of minimum weight in  $C_2'$  are outside of  $C_1'$ . Thus,  $\text{wt}(C_1^\perp \setminus C_2') = d(C_1^\perp)$ . As  $d(C_2^\perp) < d(C_1)$ , then all codewords of minimum weight in  $C_1'$  are outside of  $C_2'$ . Thus,  $\text{wt}(C_2'^\perp \setminus C_1) = d(C_2^\perp)$ . We obtain  $\delta(Q') = \min\{\text{wt}(C_1^\perp \setminus C_2'), \text{wt}(C_2'^\perp \setminus C_1)\} = \min\{d(C_1^\perp), d(C_2^\perp)\} = d(C_1^\perp) = \delta(Q)$ .  $\square$

*Example 5.4:* Let  $\mathcal{S} = S_1 \times S_2 \subseteq \mathbb{F}_q^2$  and  $g(x, y) = g_1(x)g_2(y) \in \mathbb{F}_q[x, y]$ , where  $g(s_1, s_2) \neq 0$  for all  $(s_1, s_2) \in \mathcal{S}$ . Define the tensor product

$$T(\mathcal{S}, g) = \text{RS}(S_1, g_1) \otimes \text{RS}(S_2, g_2),$$

where  $\text{RS}(S_i, g_i) = \{(f(s)/g_i(s))_{s \in S_i} \mid f \in \mathbb{F}_q[x], \deg f < \deg g_i\}$  for  $i = 1, 2$ . Note that  $\text{RS}(S_i, g_i)$  is a generalized Reed-Solomon code with evaluation points in  $S_i$ , dimension  $\deg(g_i)$ , and multipliers  $1/g_i(s)$ ,  $s \in S_i$ . In [25], the authors used the codes  $T(\mathcal{S}, g)$  to build entanglement-assisted quantum error-correcting codes with new parameters with respect to the literature. In Table I, we build LCD codes exhibiting the same set of parameters. But then, by computing the dual of the square (using [3]), we prove that there is a  $\lambda \in (\mathbb{F}_q^*)^n$  such that  $C^\perp \subseteq \lambda \star C$  for any of these LCD codes. Thus, Proposition 4.5 enables us to increase the hull, and Theorem 3.3 allows us to vary the parameter  $c$  between 0 and  $n - k$ , where  $k$  is the dimension of the code. Other works related to tensor products and quantum codes are [11], [18], and [30].

Table I shows that by puncturing  $T(\mathcal{S}, g)$ , which is the dual of a multivariate Goppa code [25], and using Theorem 3.3, we can fill in some gaps or improve the minimum distance or the dimension of some of the best-known EAQECCs recently published by Sok [36]. Other recent related work appears in [10] and [35].

We now show the existence of entanglement-assisted quantum MDS codes for  $q > 2$  and  $1 < n \leq q + 1$ . An  $[[n, \kappa, \delta; c]]_q$ -quantum code with  $\delta - 1 \leq \frac{n}{2}$  satisfying

$$2(\delta - 1) = n - \kappa + c$$

TABLE I

NEW EAQECCS. HERE,  $\mathbb{F}_q^* = \langle a \rangle$  FOR EVERY ROW; THE ELEMENTS OF  $\mathbb{F}_q$  ARE ORDERED  $0, a^0, \dots, a^{q-2}$ ; THE ELEMENTS OF  $S = \mathbb{F}_q \times \{a^1, a^2, \dots, a^i\}$  ARE ORDERED BY  $(0, a^1), (a^0, a^1), \dots, (a^{q-2}, a^2), \dots, (0, a^i), (a^0, a^i), \dots, (a^{q-2}, a^i)$ ; AND GENERATOR MATRIX COLUMNS ARE ORDERED USING THE ELEMENTS IN  $S$

Field	$S$	$g(x, y)$	Puncturing in the following entries	Parameters	Values for $h$
$\mathbb{F}_8$	$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^2 + x + a^5)(y)$	$\{8, \dots, 15\}$	$[[8, 2 - h, 6; 6 - h]]_8$	$0 \leq h \leq 2$
$\mathbb{F}_8$	$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^2 + x + a^5)(y)$	$\{10, \dots, 16\}$	$[[9, 2 - h, 7; 7 - h]]_8$	$0 \leq h \leq 2$
$\mathbb{F}_8$	$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^2 + x + a^5)(y)$	$\{11, \dots, 16\}$	$[[10, 2 - h, 8; 8 - h]]_8$	$0 \leq h \leq 2$
$\mathbb{F}_8$	$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^2 + x + a^5)(y)$	$\{12, \dots, 16\}$	$[[11, 2 - h, 9; 9 - h]]_8$	$0 \leq h \leq 2$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^2 + x + a^3)(y)$	$\{19, \dots, 32\}$	$[[18, 2 - h, 16; 16 - h]]_{16}$	$0 \leq h \leq 2$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^2 + x + a^3)(y)$	$\{21, \dots, 32\}$	$[[20, 2 - h, 18; 18 - h]]_{16}$	$0 \leq h \leq 2$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^2 + x + a^3)(y)$	$\{23, \dots, 32\}$	$[[22, 2 - h, 20; 20 - h]]_{16}$	$0 \leq h \leq 2$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)(y)$	$\{26, \dots, 32\}$	$[[25, 3 - h, 21; 20 - h]]_{16}$	$0 \leq h \leq 3$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)(y)$	$\{28, \dots, 32\}$	$[[27, 3 - h, 23; 24 - h]]_{16}$	$0 \leq h \leq 3$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)(y)$	$\{30, \dots, 32\}$	$[[29, 3 - h, 25; 26 - h]]_{16}$	$0 \leq h \leq 3$
$\mathbb{F}_{16}$	$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)(y)$	$\{32\}$	$[[31, 3 - h, 27; 28 - h]]_{16}$	$0 \leq h \leq 3$
$\mathbb{F}_{25}$	$\mathbb{F}_{25} \times \{a^1, a^2, a^3\}$	$(x^3 + a)(y)$	$\{60, \dots, 75\}$	$[[59, 3 - h, 53; 56 - h]]_{25}$	$0 \leq h \leq 3$
$\mathbb{F}_{49}$	$\mathbb{F}_{49} \times \{a^1, \dots, a^4\}$	$(x^3 + a)(y)$	$\{168, \dots, 196\}$	$[[167, 3 - h, 159; 164 - h]]_{49}$	$0 \leq h \leq 3$
$\mathbb{F}_{49}$	$\mathbb{F}_{49} \times \{a^1, \dots, a^4\}$	$(x^3 + a)(y)$	$\{175, \dots, 196\}$	$[[174, 3 - h, 166; 171 - h]]_{49}$	$0 \leq h \leq 3$

TABLE II

CONDITIONS THAT GUARANTEE THE EXISTENCE OF AN  $[[n, n - k - h, k + 1; k - h]]_q$  EAQMDS CODE FOR  $k \leq n/2$  AND FOR ANY  $0 \leq h \leq k$

Conditions	Reference
$q > 3, k \leq m \leq n/2$ , and exists a self-orthogonal $[n, m]$ GRS code.	[14]
$q > 3, n < q$ , and exists a self-orthogonal $[n + 1, k]$ extended GRS code.	[14]
$q = p^m, e \leq m, n (q - 1)$ and $k \leq \frac{p^e + n - 1}{p^e + 1}$ or $n (p^e - 1)$	[7]
$q = p^m$ odd, $e \leq m - 1, n \leq p^e$ , and $2e m$ .	[7]
$q = p^m > 3, p$ odd prime, $n = p^r, r m$ , and $2n - k - q - 2 \geq h \geq 0$ .	[38]
$q = p^m > 3, p$ odd prime, $p n, (n - 1) (q - 1)$ , and $2n - q < k + 1$ .	[38]
$q > 2$ even and $1 < n \leq q + 1$ .	[26]
$q > 3$ odd, $n = q + 1$ , and $k = \frac{q+1}{2}$ .	[26]
$q > 3$ odd, $n > 2, (n - 1) (q - 1)$ , and $-(n - 1)$ is a square in $\mathbb{F}_q$ .	[26]
$q > 2$ and $1 < n \leq q + 1$ .	Theorem 5.5

is called an *EAQMDS code*. EAQMDS codes for  $\delta > \frac{n}{2} + 1$  exist, but since we are considering codes derived from the CSS Construction, we are concerned about codes with the mentioned restriction. For more on the quantum Singleton type bounds and EAQMDS codes, see [17].

Constructions in Theorem 2.5 and 2.6 give rise to EAQECCs codes if  $C_1$  and  $C_2$  are MDS codes of the same rate in the CSS construction, or  $C$  is a Hermitian MDS code. Many constructions for EAQMDS codes have relied on the CSS or the Hermitian constructions, so there is a vast literature on how to find MDS codes with specific Euclidean, Hermitian, or Galois hull [7], [13], [14], [26], [38]. Table II exhibits some of the EAQMDS codes previously reported, which were based on the possibility of finding a proper isometry of an MDS code to get  $\text{rank}(GI_{\lambda^2}G^T) = k - h$ , where  $G$  is a generator matrix. These results complement those on unassisted ( $c = 0$ ) quantum MDS codes [19], [33]. As a generalization, we get the following result as a consequence of Theorem 4.6.

**Theorem 5.5:** If  $q > 2, 1 < n \leq q + 1$ , and  $1 \leq k \leq n/2$ , then there is an

$$[[n, n - k - h, k + 1; k - h]]_q$$

EAQMDS code for any  $0 \leq h \leq k$ .

*Proof:* Let  $C$  be a (possibly extended or double extended) generalized Reed-Solomon code of dimension  $k$ . It is known that  $C^\perp$  is a generalized Reed-Solomon code of dimension  $n - k$ . Thus, there is  $\lambda \in (\mathbb{F}_q^*)^n$  such that  $C \subseteq (\lambda \star C)^\perp$ , or equivalently,  $\dim \text{Hull}_{\lambda \star C}(C) = k$ . Applying Theorem 3.3 to  $C_1 = C$  and  $C_2 = \lambda \star C$ , we get the result.  $\square$

**Remark 5.6:** For  $k > n/2$ , we have a similar result to Theorem 5.5. In fact, if  $q > 2, 1 < n \leq q + 1$ , and  $k > n/2$ , then there is an

$$[[n, n - k - h, k + 1; k - h]]_q$$

EAQECC code for any  $0 \leq h \leq k$ , but this quantum code is not necessarily an EAQMDS code.

Theorem 5.5 can also be extended to other families of QMDS codes ( $c = 0$ ) built with the Hermitian construction. Indeed, by reducing the Hermitian hull, the existence of an EAQMDS of length  $n \leq q^2 + 1$  can be derived from the existence of a Hermitian self-orthogonal MDS code (see [27]). Such MDS codes have been reported in [19] and [33]. Since QMDS are known to be pure [22], we can apply the propagation rules in [17] to puncture QMDS with no assistance to get EAQMDS codes of shorter lengths.

## VI. FINAL REMARKS

Given two codes  $C_1$  and  $C_2$ , we studied the relative hull of  $C_1$  with respect to  $C_2$ , which is the intersection  $C_1 \cap C_2^\perp$ . We showed that the  $e$ -Galois relative hull is a particular case of the Euclidean relative hull. We proved that the dimension of the relative hull can always be repeatedly reduced by one by replacing any of the two codes with a monomially equivalent one. The proof illustrates and explains how to construct such an equivalent code. Similarly, we gave conditions under which the dimension of the relative hull can be increased by one via equivalent codes. We showed some consequences of the relative hull on quantum codes and proved the existence of some quantum MDS codes via the CSS construction.

## ACKNOWLEDGMENT

The authors were in residence at the Institute for Computational and Experimental Research in mathematics in providence, RI, or participated remotely, during the Collaborate@ICERM Quantum Error Correction Program. They also thank Rodrigo San-José for their comments and suggestions on this article.

## REFERENCES

- [1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, May 2001.
- [2] T. Ball et al., "Coding theory package for Macaulay2," *J. Softw. Algebra Geometry*, vol. 11, no. 1, pp. 113–122, Dec. 2021.
- [3] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, Sep. 1997.
- [4] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.
- [5] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
- [6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.
- [7] M. Cao, "MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction," *IEEE Trans. Inf. Theory*, vol. 67, no. 12, pp. 7964–7984, Dec. 2021.
- [8] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over  $\mathbb{F}_q$  are equivalent to LCD codes for  $q > 3$ ," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3010–3017, Jan. 2018.
- [9] H. Chen, "On the hull-variation problem of equivalent linear codes," *IEEE Trans. Inf. Theory*, vol. 69, no. 5, pp. 2911–2922, May 2023.
- [10] J. Fan, J. Li, Y. Zhou, M.-H. Hsieh, and H. V. Poor, "Entanglement-assisted concatenated quantum codes," *Proc. Nat. Acad. Sci. USA*, vol. 119, no. 24, Jun. 2022, Art. no. e2202235119.
- [11] J. Fan, Y. Li, M.-H. Hsieh, and H. Chen, "On quantum tensor product codes," *Quantum Inf. Comput.*, vol. 17, nos. 13–14, pp. 1105–1122, Nov. 2017.
- [12] Y. Fan and L. Zhang, "Galois self-dual constacyclic codes," *Des., Codes Cryptogr.*, vol. 84, no. 3, pp. 473–492, Sep. 2017.
- [13] W. Fang, F.-W. Fu, L. Li, and S. Zhu, "Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3527–3537, Jun. 2020.
- [14] X. Fang, M. Liu, and J. Luo, "On Euclidean hulls of MDS codes," *Cryptogr. Commun.*, vol. 13, no. 1, pp. 1–14, Jan. 2021.
- [15] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Inf. Process.*, vol. 18, no. 4, p. 116, Apr. 2019.
- [16] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Correction to: entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Inf. Process.*, vol. 20, no. 6, p. 216, Jun. 2021.
- [17] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of singleton bounds for quantum error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 6, pp. 3942–3950, Jun. 2022.
- [18] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 1018–1022.
- [19] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1104–1108.
- [20] D. R. Grayson and M. E. Stillman, "Macaulay2, a software system for research in algebraic geometry," 2002.
- [21] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Des., Codes Cryptogr.*, vol. 86, no. 1, pp. 121–136, Jan. 2018.
- [22] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.
- [23] H. Liu and X. Pan, "Galois hulls of linear codes over finite fields," *Des., Codes Cryptogr.*, vol. 88, no. 2, pp. 241–255, Feb. 2020.
- [24] X. Liu, H. Liu, and L. Yu, "New EAQEC codes constructed from Galois LCD codes," *Quantum Inf. Process.*, vol. 19, no. 1, pp. –1, Jan. 2020, Art. no. 15.
- [25] H. H. López and G. L. Matthews, "Multivariate Goppa codes," *IEEE Trans. Inf. Theory*, vol. 69, no. 1, pp. 126–137, Jan. 2023.
- [26] G. Luo, X. Cao, and X. Chen, "MDS codes with hulls of arbitrary dimensions and their quantum error correction," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2944–2952, May 2019.
- [27] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling, "Constructing quantum error-correcting codes that require a variable amount of entanglement," *Quantum Inf. Process.*, vol. 23, no. 1, p. 4, Dec. 2023.
- [28] G. Luo, M. F. Ezerman, and S. Ling, "Entanglement-assisted and subsystem quantum codes: New propagation rules and constructions," 2022, *arXiv:2206.09782*.
- [29] J. MacWilliams, "Error-correcting codes for multiple-level transmission," *Bell Syst. Tech. J.*, vol. 40, no. 1, pp. 281–308, Jan. 1961.
- [30] P. J. Nadkarni and S. S. Garani, "Entanglement assisted binary quantum tensor product codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2017, pp. 219–223.
- [31] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999.
- [32] A. Ravagnani, "Generalized weights: An anticode approach," *J. Pure Appl. Algebra*, vol. 220, no. 5, pp. 1946–1962, 2016.
- [33] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed–Muller codes," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 1023–1027.
- [34] M. Shibata and R. Matsumoto, "Advance sharing of quantum shares for quantum secrets," 2023, *arXiv:2302.14448*.
- [35] L. Sok, "A new construction of linear codes with one-dimensional hull," *Des., Codes Cryptogr.*, vol. 90, no. 12, pp. 2823–2839, Dec. 2022.
- [36] L. Sok, "On linear codes with one-dimensional Euclidean hull and their applications to EAQECCs," *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4329–4343, Jul. 2022.
- [37] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Royal Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, pp. 2551–2577, Nov. 1996.
- [38] G. Wang and C. Tang, "Application of GRS codes to some entanglement-assisted quantum MDS codes," *Quantum Inf. Process.*, vol. 21, no. 3, p. 98, Mar. 2022.
- [39] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 6, Jun. 2008, Art. no. 064302.

**Sarah E. Anderson** received the B.S. degree in mathematics from Presbyterian College and the Ph.D. degree in mathematical sciences from Clemson University. She is currently an Associate Professor with the Department of Mathematics, University of St. Thomas. Her research interests include coding theory and graph theory.

**Eduardo Camps-Moreno** received the B.S. and Ph.D. degrees in mathematics and physics from Instituto Politécnico Nacional, Mexico City. He is currently a Presidential Post-Doctoral Fellow with Virginia Tech. His research interests include algebra and coding theory.

**Hiram H. López** (Senior Member, IEEE) received the B.S. degree in applied mathematics from the Autonomous University of Aguascalientes and the Ph.D. degree in mathematics from CINVESTAV-IPN. He is currently an Assistant Professor with the Department of Mathematics, Virginia Tech. He held positions as an Assistant Professor with Cleveland State University and a Post-Doctoral Fellow with Clemson University. His research interests include coding theory, commutative algebra, and image processing.

**Gretchen L. Matthews** (Senior Member, IEEE) received the B.S. degree in mathematics from Oklahoma State University, the M.B.A. degree from Virginia Tech, and the Ph.D. degree in mathematics from Louisiana State University. She was a Faculty Member with Clemson University. She is currently a Professor of mathematics with Virginia Tech and the Director of a regional component of the Commonwealth Cyber Initiative (CCI). She held a Post-Doctoral appointment with The University of Tennessee. Her research interests include algebraic geometry and combinatorics and their applications to coding theory and cryptography.

**Diego Ruano** received the dual M.S. degree in mathematics from the University of Valladolid, Spain, in 2002, and the University of Kaiserslautern, Germany, in 2003, and the Ph.D. degree in mathematics from the University of Valladolid in 2007. He was a Post-Doctoral Researcher with the University of Kaiserslautern in 2007 and a H. C. Ørsted Post-Doctoral Fellow with the Technical University of Denmark in 2008. From 2009 to 2012, he was an Assistant Professor and an Associate Professor with Aalborg University, Denmark, from 2013 to 2018. He was a Ramón-y-Cajal Fellow with the University of Valladolid. He is currently an Associate Professor of mathematics with IMUVA-Mathematics Research Institute, University of Valladolid. His research interests include algebraic geometry and computer algebra, and their applications to classical and quantum coding theory and cryptography.

**Ivan Soprunov** received the M.S. degree in mathematics and applied mathematics from Moscow State University and the Ph.D. degree from the University of Toronto. He was a Visiting Assistant Professor with the University of Massachusetts, Amherst, MA, USA. He is currently a Professor with the Department of Mathematics and Statistics, Cleveland State University. His research interests include computational algebraic geometry and its applications to combinatorics and coding theory.